# EXHIBIT 13
# (Excerpted)

US008533469B2

(12) **United States Patent**
**Song et al.**

(10) **Patent No.: US 8,533,469 B2**
(45) **Date of Patent: Sep. 10, 2013**

(54) **METHOD AND APPARATUS FOR SHARING DOCUMENTS**

(75) Inventors: **Zhexuan Song**, Silver Spring, MD (US); **Ryusuke Masuoka**, Potomac, MD (US); **Jesus Molina**, San Francisco, CA (US)

(73) Assignee: **Fujitsu Limited**, Kawasaki-shi (JP)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 711 days.

(21) Appl. No.: **12/623,861**

(22) Filed: **Nov. 23, 2009**

(65) **Prior Publication Data**

US 2011/0126008 A1 May 26, 2011

(51) **Int. Cl.**
***H04L 29/00*** (2006.01)

(52) **U.S. Cl.**
USPC ..... **713/167**; 713/164; 709/225; 709/226

(58) **Field of Classification Search**
USPC ..... 713/164
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 6,314,425 | B1 * | 11/2001 | Serbinis et al. | 1/1 |
| 6,978,366 | B1 * | 12/2005 | Ignatchenko et al. | 713/166 |
| 2003/0056095 | A1 * | 3/2003 | Elliott et al. | 713/164 |
| 2008/0002830 | A1 * | 1/2008 | Cherkasov et al. | 380/277 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| WO | WO 2008/042846 | 4/2008 |

OTHER PUBLICATIONS

International Search Report and Written Opinion; PCT/US2010/055194; pp. 11, Jan. 7, 2011.

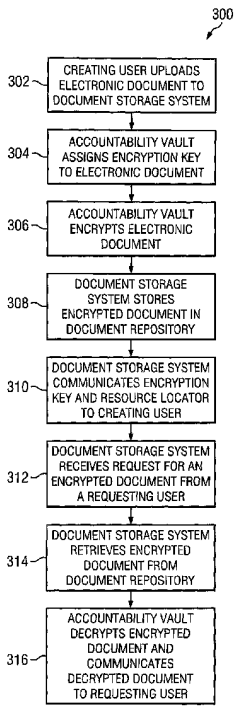
* cited by examiner

*Primary Examiner* — Phillip J. Chea
*Assistant Examiner* — Ghazal Shehni
(74) *Attorney, Agent, or Firm* — Baker Botts L.L.P.

(57) **ABSTRACT**

A method for securely sharing electronic documents on a document storage system. The method includes receiving an electronic document from a creating user, generating an encryption key unique to the electronic document, encrypting the electronic document using the encryption key to create an encrypted electronic document, and communicating the encrypted electronic document to a document repository for storage/ The method also includes identifying a resource locator for uniquely identifying the storage location of the encrypted electronic document and communicating the encryption key and the resource locator to the creating user. The method also includes receiving the encryption key and the resource locator from a requesting user, retrieving the encrypted electronic document from the document repository using the resource locator, decrypting the encrypted electronic document using the encryption key, and communicating the decrypted electronic document to the requesting user.

**16 Claims, 2 Drawing Sheets**



106 of electronic document sharing system 100 may refer to a person acting as an end user or to the device or devices used by such a person to access electronic document sharing system 100, such as a personal computer, kiosk, or mobile computing device.

In general, the components of electronic document sharing system 100 may securely store an electronic document edited by a user 106 such that the user 106 and other authorized users 106 may later access that electronic document in a manner that provides the appropriate encryption key only to authorized users and does not store the encryption key within document storage system 108. User 106 may create a document and communicate that document to document storage system 108 via any appropriate network, such as the internet or a private intranet. Accountability vault 102 of document storage system 108 may then encrypt the electronic document using an appropriate encryption scheme, as described in more detail below with reference to FIG. 2. Once encrypted, the electronic document may then be stored in document repository 104. Document repository 104 may be any appropriate database and/or database management system suitable for use in a networked document sharing system, such as Oracle Database or IBM's DB2.

Accountability vault 102 may also communicate the encryption key for the electronic document to the user that created the document ("creating user"), as well as a resource locator. The creating user may be the user 106 that actually created the electronic document or a user 106 that has edited the document or otherwise gained access to the document and now desires to store the document on document storage system 108.

The resource locator may be a reference associated with the electronic document that would allow user 106 to locate or request access to the electronic document. In some embodiments, document storage system 108 may be web-enabled, with each electronic document stored in document repository 104 assigned a unique uniform resource locator ("URL"). Entering this URL into a standard web browser may allow user 106 to request access to the specific electronic document. In some embodiments, the encryption key and the resource locator are communicated to user 106 in a text format. Communication in this manner may allow user 106 to share this information with other users 106 in a convenient manner. Communication of the key and the resource locator between document storage system 108 and user 106, or between user 106 and another user 106 may be in any appropriate format, such as email or SMS.

In some configurations, it may be most efficient to combine the resource locator and encryption key into a single line of communication. In other configurations, it may be deemed to be more secure to separate the resource locator and encryption key into separate communications. In those configurations favoring utmost efficiency, a single communication such as a single URL may be preferable. For instance, the URL communicated to user 106 may take the form of location+resource locator+encryption key. In a web-enabled environment such as that described above, this may take the illustrative form of:

http://web_host/retrieve_document?
doc_id=1234&key=19da301afe0231823

In this illustrative example, "web_host" may be the network location of database storage system 108, "retrieve_document" may be the name of a process executable on database storage system 108 used to retrieve the desired electronic document, "doc_id" may be the resource locator unique to the desired electronic document, "1234" may be the value of the resource locator, "key" may be the identification of the encryption key used by the "retrieve_document" process, and "19da301afe0231823" may be the value of the encryption key unique to the desired electronic document. This example has been offered solely to facilitate understanding of FIG. 1, and in no way should be interpreted to limit the teaching of this disclosure.

In other embodiments, user 106 may be able to identify other users 106 who should receive the resource locator and encryption key when user 106 stores an electronic document on document storage system 108. Once informed, accountability vault 102 may, in some embodiments, communicate the resource locator and encryption key directly to other users 106 whom user 106 has previously identified. This communication may take the same form as the communication to user 106 described above.

User 106 in possession of the resource locator and encryption key may, at an appropriate time, communicate with document storage system 108 in an attempt to retrieve the electronic document associated with that resource locator and encryption key. In some embodiments, accountability vault 102 may receive the resource locator and encryption key from user 106, retrieve the identified document from document repository 104, and decrypt the document using the encryption key. Once decrypted, accountability vault 102 may communicate the unencrypted document to the requesting user 106.

Importantly, in the disclosed embodiments, the encryption key is never stored within document storage system 108 except to the extent required to execute the encryption and decryption of the stored electronic document. This allows improvements in the security of the contents of the electronic documents stored within document storage system 108. For instance, administrators or other users with high-level privileges for document storage system 108 may not be able to read the encrypted electronic documents stored in document repository 104.

FIG. 2 is a simplified block diagram illustrating various functional components of document storage system 108, in accordance with certain embodiments of the present disclosure. The illustrated document storage system 108 may include accountability vault 102, document repository 104, policy engine 106, and audit engine 110. The various components of document storage system 108 may be, in some embodiments, a software program stored on computer-readable media and executable by a processor of document storage system 108. For clarity of description, FIG. 2 depicts the components as separate modules. In some embodiments, the components may be stand-alone software programs. However, the components may also be a component or subroutine of a larger software program, or hard-coded into computer-readable media, and/or any hardware or software modules configured to perform the desired functions.

Accountability vault 102 may be configured to encrypt and decrypt an electronic document in response to communication from a user 106, as described in more detail above with reference to FIG. 1. In some embodiments, the encryption algorithm used by accountability vault 102 to create the encryption key may be any encryption algorithm configured to produce an encryption key unique to the electronic document and randomly generated. The Advanced Encryption Standard (AES) provides a well-known example of such an encryption algorithm.

In some embodiments, the encrypted documents are stored in document repository 104. Document repository 104 may be any appropriate computer-readable memory such as a database and/or database management system suitable for use in a networked document sharing system, such as Oracle